OhioDAS Department of Administrative Services | Office of Information Technology

Data Breaches: How to Prepare and Respond

Matt Williams

Agency Chief Information Security Officer, Assigned to Department of Education

matthew.williams@das.ohio.gov

OhioDAS Office of Information Technology | Office of Information Security and Privacy
Service · Support · Solutions

Headlines

Yukon Public Schools hit with data breach
W-2 Scam
FOX 25 News, Oklahoma, March 2nd 2017

After data breach, Md. school district passes new policy to handle stolen information
Frederick News Post, February 22, 2017

OhioDAS Office of Information Technology | Office of Information Security and Privacy
Service · Support · Solutions

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

How to prepare for a breach

- Education and awareness program
- Determine roles for planning
- Develop a plan
- Regular event simulations

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Components of a plan

- Inventory of PII (Personally Identifiable Information) and other sensitive data.
- Inventory of service providers that use or manage PII and other sensitive data
- Notification and escalation path
- Defined roles for incident handling
- Policies and procedures for data handling and incident handling

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Inventory of data and systems

- Categorize the type of individuals you collect data about (students, employees, volunteers, vendors?)
- Identify the types of data you collect about each category (SSN, BCI/FBI, medical/health information, financial data)
- Identify all compliance requirements (FERPA, HIPAA, State, and local)

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Inventory of data and systems (cont.)

- Where is relevant information stored (paper, PCs, servers, databases, applications, backup tapes, removable media)
- What data is encrypted in transit and at rest (PCs, server file systems, databases, applications, email, wireless networks)
- What access controls are in place (file systems, database, applications)
- What PII or sensitive data collected, stored, transmitted, or otherwise handled by a third party provider

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Inventory of data and systems (cont.)

- Is access to PII and sensitive data limited and monitored and logged to ensure data is only accessed by authorized individuals. Is access authorization documented and periodically reviewed?
- Which systems and databases have access logging in the event of a breach? Would the logging indicate who accessed or made changes and what data was changed?
- Are there third party contractual requirements that mandate notification of a breach?

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

People and Roles for notification incident handling

- Identify the person or group responsible for implementing privacy and data security policies and procedures
- Identify points of contact that are involved in the event of a breach from the following areas: Legal Counsel, Communications, Privacy/Compliance, Information Technology, Security, Human Resources, Administration

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Notification

- Document the incident notification path
  - Escalation path from person who identified the breach through the Superintendent
- Document the compliance notification plan
  - Who determines when a third party is notified based on the data that is compromised (generally legal).
  - Document standard types of remediation offered and notification templates

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Law enforcement notification

- Some breaches require the notification of local, state, and/or federal law enforcement.
- Leverage your legal counsel to determine which data requires notification to which authorities

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Recommended Policies and Procedures

- Information Handling – How PII and sensitive data should be handled. What types of media are permitted.
- Data Classification – Classification provides for consistent handling of information, no matter what form it takes, where it goes, or who possesses it.
- Privacy Policy – Identifies why data is collected and used and how the someone can see the data stored on them and make corrections.
- Encryption – How data and systems are encrypted. Includes all data, systems, servers, PCs & Notebooks, and mobile devices (smartphones & tablets).

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Recommended Policies and Procedures

- Password policy – Identifies how passwords are constructed, used, and changed.
- Incident response – What procedurally occurs in the event of a breach or incident.
- Acceptable use – Identifies how employees are allowed to use data and systems. Establish least privileged access policy.

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Incident Response Actions

1. Contain the data breach
2. Carry out the notification and escalation plan
3. Analyze the breach
4. Analyze the legal implications of the breach
5. Contact law enforcement
6. Contact insurance carrier if applicable
7. Organize public inquiry plan if applicable
8. Determine remediation strategy

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Information to collect immediately after the breach

- Date, time, duration, location of breach
- How the breach was discovered, by whom, and any other details (how breach occurred, entry points, paths taken, whether data was deleted, modified, or viewed, whether any devices are missing)
- Details about the compromised data (list of affected individuals, data fields, number of records and if data was encrypted)

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Complete a root cause analysis with lessons learned

- Determine the cause of the data breach
- Identify how the weakness was able to be exploited
- Identify ways to prevent the same type of breach again.

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Incident Response and Reporting

US Department of Homeland Security Cyber Security Division
Through proactive monitoring they are able to inform state and local government organizations about potential and in process incidents:
- •Website defacement
- •Cyber-threats against a school, state, or local government entities

Ohio Department of Homeland Security – Fusion Center 877-OHS-INTEL
Incident Response:
- •Cyber attack that has occurred or is occurring
- •Information sharing among school, state, and local government entities
- •Advisable to report incidents – Can be done anonymously

State of Ohio Office of Information Security and Privacy (OISP) 614-644-9391
Security Program Guidance:
- •What resources available
- •Incident response
- •Proactive notification of incidents

MS – ISAC - Membership based
School districts should work through their local municipalities or Ohio OISP

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

References

The International Association of Privacy Professionals - Security Breach Response Plan Toolkit - Created by the IBM Corporation and Hogan Lovells US LLP as part of the IAPP's (The International Association of Privacy Professionals) Pro Bono Privacy Initiative
https://privacyassociation.org/

State of Ohio Office of Information Security and Privacy – 614-644-9391
State CISO David Brown
http://privacy.ohio.gov/

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions